Law Firms Are Pressed on Security for Data

nytimes.com

Yana Paskova for The New York Times Daniel B. Garrie, of the computer security consulting firm Law & Forensics, said demands from corporate clients were "forcing the law firms to clean up their acts."

A growing number of big corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount.

Wall Street banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and deter attacks from hackers bent on getting their hands on corporate secrets either for their own use or sale to others, said people briefed on the matter who spoke on the condition of anonymity. Some financial institutions are asking law firms to fill out lengthy 60-page questionnaires detailing their cybersecurity measures, while others are doing on-site inspections.

Other companies are asking law firms to stop putting files on portable thumb drives, emailing them to nonsecure iPads or working on computers linked to a shared network in countries like China and Russia where hacking is prevalent, said the people briefed on the matter. In some cases, banks and companies are threatening to withhold legal work from law firms that balk at the increased scrutiny or requesting that firms add insurance coverage for data breaches to their malpractice policies.

"It is forcing the law firms to clean up their acts," said Daniel B. Garrie, executive managing partner with Law & Forensics, a computer security consulting firm that specializes in working with law firms. "When people say, 'We won't pay you money because your security stinks,' that carries weight."

The vulnerability of American law firms to online attacks is a particular concern to law enforcement agencies because the firms are a rich repository of corporate secrets, business strategies and intellectual property. One concern is the potential for hackers to access information about potential corporate deals before they get announced. Law enforcement has long worried that law firms are not doing enough to guard against intrusions by hackers.

In 2011, the Federal Bureau of Investigation began organizing meetings with the managing partners of top law firms in New York and other major American cities to highlight the problem of computer security and corporate espionage, especially for law firms with offices in foreign countries like China and Russia.

Despite those meetings, F.B.I. officials and security experts say, law firms remain a weak link when it comes to online security. But the push from corporate clients may have more impact on changing law firm attitudes than anything else.

"Clients are putting more restrictions on law firms about things to do to protect

Matthew Coleman Mary E. Galligan, an executive at Deloitte & Touche.

themselves," said Mary E. Galligan, an executive in the cyber-risk services division of Deloitte & Touche and the former special agent in charge of cyber and special operations for the New York office of the F.B.I. "It is being driven by victims of hackers, and they don't want to be victims again. It's just good business sense."

When she was with the F.B.I., Ms. Galligan organized the meetings with managing partners of law firms to impress on them the need to better police their computer systems. The first meeting, held in New York in November 2011, was attended by top lawyers from nearly 200 firms. Over the next two years, Ms. Galligan said, she arranged half a dozen smaller meetings with law firm executives around the country. She said it had taken awhile, but she saw law firms being more proactive about computer security in large part because of the demand from clients.

Companies are prodding law firms on security at a time of overall rising concern about hacker attacks like the information breach at Target last year, when the retailer said at least 40 million credit and debit card accounts were compromised. Financial regulators are also requiring banks to make sure that vendors they rely on, like law firms, are vigilant when it comes to dealing with hackers and other online intruders.

"The public and private sectors must be riveted in lock step in addressing these threats," Mary Jo White, the chairwoman of the Securities and Exchange Commission, said Wednesday at a round-table discussion on the obligations of public companies to disclose online attacks. The discussion brought together more than two dozen security experts from the federal government and the financial services sector.

Still, spying by governments both at home and abroad and how that could involve a breach of client confidence is also a concern for businesses. In February, The New York Times reported that communications between lawyers at Mayer Brown, a big Chicago-based law firm, and officials with the Indonesian government were intercepted by an Australian intelligence agency that had ties to the National Security Agency, the federal agency that has been under siege for nearly a year because of its domestic spying program. The American Bar Association, with nearly 400,000 members, sent a letter to the N.S.A. to say it was incumbent on the security agency to make sure the principle of attorney-client privilege was protected.

Stuart Pattison, a senior vice president with Endurance Specialty Holdings, an underwriter of professional liability insurance coverage for law firms, said the main concern for the F.B.I. was state-sponsored hackers breaching a law firm computer system to tap into information about what American corporations were doing. He said that a few law firms had recently inquired about obtaining an added level of insurance coverage for data breaches in response to a demand from their corporate clients.

Despite the concern, it's hard to gauge just how vulnerable law firms are to attacks from hackers. There are few rules requiring firms to make public any breaches, and because the firms have little direct interaction with consumers, there is no need for them to publicly report a hacking incident the way a bank or a retailer would. In 2012, Mandiant, a security consulting firm, put out a report estimating that 80

percent of the 100 largest American law firms had some malicious computer breach in 2011. Actual reports of confidential information hacked from a law firm computer system and later winding up on some overseas server are rare, however.

Representatives for several large law firms, all of whom declined to discuss the topic publicly, said privately that the threat assessments from the F.B.I. and consulting firms were overstated. The law firm representatives said hacker attacks were usually email “phishing” schemes seeking to access personal information or account passwords, the kind of intrusions that have become commonplace and are easily contained.

But Vincent I. Polley, a lawyer and co-author of recent book for the American Bar Association on cybersecurity, said many law firms were not even aware they had been hacked. He said a lot of law firm managers were in denial about the potential threat.

“A lot of firms have been hacked, and like most entities that are hacked, they don’t know that for some period of time,” said Mr. Polley. “Sometimes, it may not be discovered for a minute or months and even years.”

A version of this article appears in print on 03/27/2014, on page B1 of the NewYork edition with the headline: Law Firms Are Pressed an Security for Data.